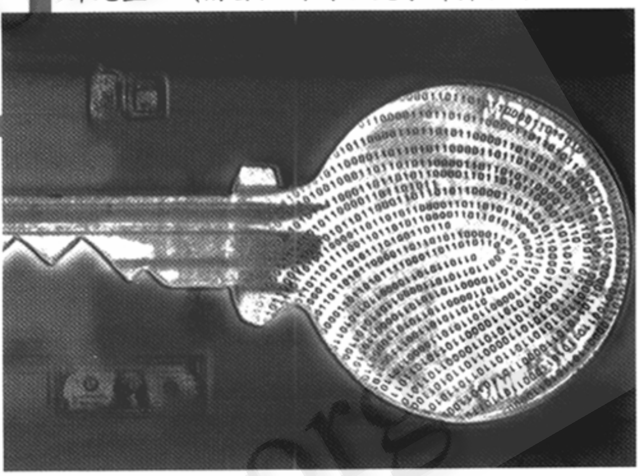
构建企业安全电子邮件体系

摘要：本文详细介绍了应用Windows 2000技术，实现安全电子邮件体系的基本过程。包括认证中心的建立与管理，数字证书的申请，以及安全电子邮件操作。

关键词：安全电子邮件 公开密钥体制 数字证书 认证中心

钟元生 （南昌江西财经大学计算机系 330013）



1 概述

公开密钥机制是电子商务的一种重要技术，安全电子邮件即为其应用之一。迄今为止，各类文章主要在于理论介绍，具体实现介绍比较少见。实际上，本文介绍利用Windows 2000实现的基本方法。为便于大家掌握，以下介绍采用最简单的工作环境，即：Windows 2000作为服务器操作系统，同时安装证书颁发机构(Certificate Authority ,CA)高级服务组件，浏览器用IE4.0或IE5.0，E-mail软件用Outlook Express，服务器放在Intranet上，IP地址为10.15.11.13，通过网络颁发数字证书。企业安全电子邮件体系示例模型见图1。

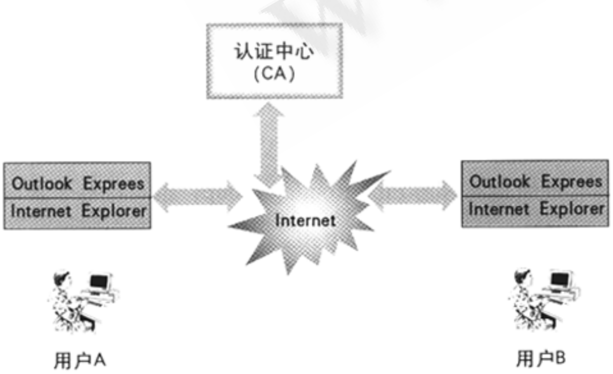


图 1 企业安全电子邮件体系示例模型

2 认证中心的建立与管理

2.1 安装证书颁发机构

(1) 启动Windows 2000后，在Windows 2000配置您的服务器对话框中，单击右下方的高级下拉列表，单击可选组件，再单击中间的启动Windows组件向导。

(2) 在Windows组件向导对话框中，选择组件列表中证书服务，然后单击下一步按钮，由向导按您的设置自动安装，安装完毕后，返回到Windows配置您的服务器对话框。

2.2 启动证书颁发机构

依次选择菜单命令开始／程序／管理工具／证书颁发机构，即可启动Windows 2000的证书颁发机构服务。

这是一个树型管理结构，单击证书颁发机构的名称(本例为z.j.u CA，以下同)，可以打开该机构下面的四个文件夹，分别是：

(1) 吊销的证书：本CA吊销作废的证书列表

(2) 颁发的证书：本CA颁发的有效证书列表

(3) 待定申请：本CA接受的要求颁发证书，且还需审查的申请列表

(4) 不成功的申请：被本CA拒绝接受的证书申请列表

2.3 配置证书颁发策略

单击证书颁发机构名称，依次选择菜单命令操作/属性，出现z.j.u CA属性对话框，再在对话框中单击策略模块页标签，单击下方的配置按钮，显示属性设置对话框，在其中设置默认操作为以下之一：

(1) 将证书申请状态设定为待定：此时CA接受证书申请，但颁发必须由系统管理员检查待定申请，用手工颁发，该方式有利于对证书申请进行人工审查。

(2) 始终颁发证书：CA接受申请后，由服务器自动颁发证书，而不放入待定申请列表中。

(3) 一般将证书申请状态设定为待定，以便于控制。选定了默认操作后，单击两次确定按钮，回到证书颁发机构，颁发策略就配置好了。

2.4 证书颁发、吊销与显示

(1) 颁发证书。用户在浏览器中通过专门的证书服务Web页，向认证中心提出申请，再由系统管理员审查申请人的资格，给申请人发放数字证书，而申请人再在浏览器端下载证书。随后，申请人就可以凭着这一证书，向Internet上其他人证明自己的身份。

当认证中心(CA)的颁发策略为始终颁发证书时，系统管理员不用另外操作以专门颁发，而由系统自动颁发。但用于重要场合的证书，一般应由系统管理员审查申请人的身份，再决定是否颁发。常常检查申请人在现实世界中的有效证件，如身份证、营业执照，甚至银行存折等，以保证证书的权威性，人工颁发的方法是：

单击待定申请列表中某一行，再右击鼠标，出现弹出菜单后，再选择所有任务／颁发命令。颁发的证书在颁发证书列表中可以查看到，同时从待定申请中删除该条目。申请者可以通过证书服务Web页下载自己的证书。(参见第三部分)

若选择弹出菜单中所有任务／拒绝命令，则用户申请不成功，申请条目移入不成功的申请列表中。

(2) 吊销证书。因某种原因（如密码丢失或证书有人盗用等），用户可以向系统申请吊销证书。系统管理员在颁发的证书列表中，找到指定的证书所在行，右击鼠标，在弹出菜单中选择所有任务／吊销，该证书即被吊销，其他用户可以通过下载CA的证书吊销表(Certificate Revoked List; CRL)来检查接到的证书的有效性。

(3) 显示证书细节。为了显示证书的细节，只要找到指定的证书行，并双击它，即可打开证书对话框(见图2)。在这个对话框中，含常规、详细信息和证书路径三个页，可依次检查证书目的、有效日期、颁发者、颁发给谁及证书序列号、证书路径等信息，以及证书是否有问题。注意申请ID号及证书序列号是不重复的。

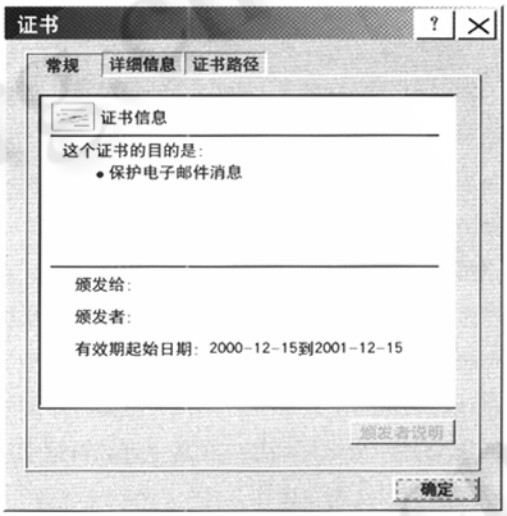


图2

3 数字证书的申请、下载与管理

这里以申请E-mail保护证书为例说明使用过程。

3.1 提交申请

启动IE4.0或IE5.0，在地址栏打入:http://10.15.11.13/certsrv ,将显示证书服务web页。这是Windows提供的一个ASP实现的证书服务模板。按照提示就可以顺利的完成申请提交、证书及证书吊销表的下载安装任务。

提交证书申请一般步骤是：

(1) 选择任务：申请证书，单击下一步；

(2) 选择申请类型：高级申请，单击下一步；

(3) 选择使用这个表格向这个CA提交一个证书申请，再单击下一步；

(4) 在高级证书申请中输入有关信息；

(5) 单击提交按钮，当出现证书挂起提示时，即完成了申请过程。

假设申请人姓名：zhyuans-cise, 电子邮件：zhyuans@cise.zju.edu.cn，意图：E-mail保护证书。并应选择启用严格密钥保护、标记密钥为可导出两个复选框。其他内容

根据实际情况设置。此时，你必须等待CA系统管理员给你颁发证书，再下载证书。

3.2 下载安装证书

① 回到证书服务起始页，选择检查挂起的证书单选项，再单击下一步；

② 出现下一个画面选择你要检查的证书申请，若CA系统管理员已经接受了你的申请，并已经颁发了一个证书，则将出现一个画面，告诉你证书已发布。

③ 单击安装此证书，系统将自动从CA下载该证书安装到你的计算机中。若没有出现该提示，则不能下载证书，你必须分析根据其中原因，要么等待，要么与系统管理员联系。

证书安装后，通过Outlook就能够检查到相应的E-mail保护证书，其他证书则可以通过IE检查。

3.3 管理证书

通过Outlook Express的有关命令来对计算机中存储的E-mail证书进行管理。其方法是：选择菜单中工具／选项命令，单击安全页标签，单击安全邮件中间的数字标识按钮，将显示证书对话框，在其中可以对证书进行查看、导入、导出及删除操作。

(1) 导出：将选中的某一证书导出，以文件的形式存储到其他位置，以便于你备份及转移到其他计算机中，例如放到家里的机器中。若在申请证书中指定标记密钥为可导出，即可将私钥导出，并可设置密钥保护级别，满足私人信息交换的要求，否则只能导出公钥。当导出私钥时，会要求你设置密码。具体操作按屏幕提示，本文略。

(2) 导入：这是导出操作的逆操作。

(3) 删除：删除指定的证书，若某一证书指定启用了严格密码保护，计算机会要求你输入密码，若密码不对，不允许删除。

(4) 查看：选中要查看的证书，双击它即可检查证书的详细情况（见图2）。

IE5.0中对证书的管理方法是：①选择工具／Internet选项命令；②打开Internet选项对话框中的内容页，单击其证书按钮；③显示证书管理器。

4 安全电子邮件操作过程

假设要在两个用户A与B之间传输机密信件，E-mail分别为zhyuans@cise.zju.edu.cn，和zhyuans@zjuem.zju.edu.cn。各自计算机分别称为机器A与机器B，两个用户均已经取得了自己的电子邮件保护证书，并存储在各自机器中。由用户A首先发起通信。

实现的一般步骤为：

(1) 用户A通过机器A向用户B发签名邮件，以传送自己的公钥给用户B：

①在机器A中，用Outlook撰写一个新邮件，收件人为zhyuans@zjuem.zju.edu.cn；

②选择工具／数字签名命令；

③单击发送工具按钮。

(2) 用户B接收自己的邮件，当选择由用户A发来的邮件时，会出现提示，告诉他收到了数字签名邮件，单击下面的继续按钮，就能显示原邮件内容。

此时，若是第一次收到用户A的签名或加密邮件的话，机器会自动将用户A的公钥证书存入用户B机器中。

(3) 用户B签名并加密发送收到邮件的确认信息给用户A，步骤是：

① 选择刚收到的邮件，单击回复作者按钮；

② 修改邮件，选择工具／加密与工具／签名命令；

③ 单击发送工具按钮。

(4) 用户A在机器A上接收到用户B的确认邮件，并发送确认信息给用户B当选择该邮件时，机器会提示收到了加密及签名邮件，单击继续按钮，若能正确显示收到的邮件内容，则表示对方确实是你要通信的人。同样，用户A的机器中也会自动存储用户B的公钥证书。

(5) 用户A回复一封加密回信给用户B。

以后，双方通信就可以对第三者保密，即实现了加密通信。若用户将证书中的私钥导出，则不再能进行加密通信，必须重新导入私钥证书恢复。

5 结束语

认证中心建立好后，还可以实现基于SSL协议(Secure Socket Layer，安全套接字层)的加密Web通信等更复杂的电子商务功能。具体过程，另文介绍。■

参考文献

1 梁晋、施仁、梁峰、彭波。Windows 2000公钥体系结构，计算机工程，2000，Vol.26 No.7：1–2，146。

2 洪琳、李展、数字签名、数字信封和数字证书，计算机应用，2000，Vol.20 No.2：41–42。

3 Liaquat Khan, Deploying Public Key Infrastructures, Information Security Technical Report, 1998, 3(2): 18–33。

4 Nick Mansfield, Designing a Practical Public key Infrastructure (PKI), Information Security Technical Report, 1999, 4(4): 18–27。